Octobre 2025

L'Analyse d'impact relative à la protection des données personnelles

Nouvel instrument introduit par la Loi n° 1.565 du 3 décembre 2024, l'analyse d'impact relative à la protection des données (AIPD ou DPIA anglais) est une étude dont l'objectif est de déterminer et d'analyser les risques qu'un traitement de données peut poser pour la vie privée des individus.

Nécessité d'un risque élevé pour les droits et libertés des personnes concernées

Toute opération qui pourrait engendrer des risques pour les droits et libertés des personnes physiques ne requiert pas automatiquement une analyse d'impact. La loi n'exige en effet une analyse d'impact que lorsqu'un traitement est susceptible d'entraîner un **risque élevé pour les droits et libertés**, notamment en cas de recours à une **nouvelle technologie de traitement**.

Qu'entend-on par nouvelle technologie de traitement ?
Selon les Lignes directrices concernant l'analyse d'impact adoptées le 4 avril 2017 par le Groupe de travail *« Article 29 »*[1], l'utilisation d'une nouvelle technologie, définie en « *conformité avec l'état des connaissances technologiques* », peut déclencher la nécessité d'une analyse d'impact, et « *ce en raison du fait que l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes* ». La réalisation d'une analyse d'impact permettra ainsi au responsable du traitement de comprendre et de traiter ce risque.

[1] Groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du Règlement Général sur la Protection des Données - RGPD).

Dans quels cas existe-il un risque élevé pour les droits et libertés des personnes concernées ?

L'article 35 de la Loi 1.565 du 3 décembre 2024 prévoit qu'un **risque élevé** existe notamment dans **4 cas** :

1er cas : l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

2ème cas : le traitement à grande échelle de données sensibles ou de données à caractère personnel relatives aux **infractions, condamnations pénales** et **mesures de sûreté** ou portant sur des **soupçons d'activités illicites**.

3ème cas : la surveillance systématique à grande échelle de zone accessible au **public**.

4ème cas : l'utilisation à grande échelle d'un identifiant numérique.

Cette liste n'est pas exhaustive comme l'atteste l'emploi du mot « *notamment* ». Aussi, d'autres opérations de traitement qui ne figurent pas dans ces 4 cas peuvent néanmoins présenter un risque aussi élevé et donc nécessiter une analyse d'impact.

Quels sont les critères permettant de déterminer si un traitement est susceptible d'entrainer un risque élevé pour les personnes concernées ?

L'article premier de l'Arrêté Ministériel n° 2025-361 du 14 juillet 2025 portant application de l'article 35 de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles établit la liste des critères permettant de déterminer si un traitement est susceptible d'engendrer un **risque élevé pour les droits et libertés** des personnes physiques. La plupart de ces critères ont été précisés par les Lignes directrices du Groupe de travail *« Article 29* ».

Ceux-ci sont au nombre de 8 :

- **Critère n° 1 : l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage**

Selon les lignes directrices du Groupe de travail « *Article 29* », il s'agit d'évaluation portant notamment sur des « *aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement ou sa localisation et ses déplacements* ».

Exemples :

- une entreprise analysant les usages ou la navigation sur son site Internet pour créer des profils comportementaux ou marketing
- un établissement financier passant ses clients au crible d'une base de données de cote de crédit ou d'une base de données dédiée à la lutte contre le blanchiment de capitaux et le financement du terrorisme

- **Critère n° 2 : la prise de décision automatisée produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire**

Pour le Groupe de travail « *Article 29* », une prise de décision exclusivement automatisée est la capacité de prendre des décisions par des moyens technologiques sans intervention humaine.

Les décisions automatisées peuvent être fondées sur n'importe quel type de données, par exemple :

• les données fournies directement par les personnes concernées (comme les réponses à un questionnaire);
• les données observées au sujet des personnes (comme les données de localisation recueillies par l'intermédiaire d'une application) ;
• des données dérivées ou inférées, comme le profil d'une personne qui a déjà été créé (par exemple une cote de solvabilité).

Ces décisions automatisées peuvent être prises avec ou sans profilage et doivent **produire des effets juridiques** à l'égard de la personne concernée ou **l'affecter de manière significative** (en entraînant par exemple l'exclusion ou une discrimination).

Exemple : création par un établissement bancaire d'une base de données spécialisée dans la notation de crédit

- **Critère n° 3 : la surveillance systématique**

Selon les lignes directrices du Groupe de travail « *Article 29* », il s'agit d'une collecte de données personnelles « *susceptible d'intervenir dans des circonstances telles que les personnes concernées ne savent pas qui collecte leurs données et de quelle façon elles seront utilisées. En outre, il peut être impossible pour les personnes de se soustraire à un tel traitement dans l'espace public (ou accessible au public) considéré* ».

Sont ainsi concernés tous les traitements ayant pour objet l'observation, la surveillance ou le contrôle des personnes concernées, y compris la collecte de données via les réseaux sociaux.

Exemples :

- l'utilisation d'un système de caméras dans une galerie commerciale
- la surveillance par un employeur de tous les e-mails sortants par le biais de remontées d'alertes

- **Critère n° 4 : le traitement de données sensibles ou relatives aux infractions, condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activité illicites**

Conformément au chiffre 9 de l'article 2 de la Loi n° 1.565 du 3 décembre 2024, les données sensibles sont *« les données à caractère personnel qui révèlent, directement ou indirectement, des opinions ou des appartenances politiques, les origines raciales ou les origines éthiques, les convictions religieuses, philosophiques ou l'appartenance syndicale, ou encore des données génétiques, des données biométriques aux fons d'identifier une personne physique de manière unique ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

Exemple : les traitements de santé réalisés par un établissement de soins

- **Critère n° 5 : le croisement ou la combinaison d'ensembles de données**

Pour le Groupe de travail « *Article 29* », ces ensembles de données peuvent être issus de deux opérations de traitement de données, ou plus, effectués à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée.

Exemple : la collecte de données sur les réseaux sociaux publics dans le but de générer des profils

- **Critère n° 6 : le traitement de données concernant des personnes vulnérables**

Selon l'exposé des motifs de la Loi n° 1.565 du 3 décembre, 2024, les personnes vulnérables doivent être entendues comme étant notamment « *en sus des enfants, les salariés, les personnes handicapées, les personnes âgées…* ».

Exemple : la collecte des données pseudonymisées de patients participant à une recherche clinique

- **Critère n° 7 : l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles**

L'utilisation d'une nouvelle technologie peut impliquer de nouvelles formes de collecte et d'utilisation des données, dont les conséquences personnelles et sociales peuvent être inconnues au moment du déploiement. Une AIPD permettra donc au responsable du traitement de comprendre et de traiter de tels risques.

Dans ses lignes directrices, le Groupe de travail « *Article 29* » donne pour exemple l'utilisation combinée de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques.

- **Critère n° 8 : le traitement empêchant la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat**

Pour le Groupe de travail « *Article 29* », ces traitements incluent notamment les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat.

Exemple : une banque passant ses clients au crible d'une base de données de cote de crédit avant de décider ou non ou leur octroyer un prêt

Dès lors qu'un traitement répond à **au moins deux de ces critères**, le responsable du traitement doit considérer que ledit traitement est **susceptible de présenter un risque élevé** pour les droits et libertés des personnes concernées et qu'**une analyse d'impact est donc nécessaire**.

Dans certains cas, toutefois, il peut estimer, compte tenu du contexte du traitement, qu'un seul critère suffit.

Cas particulier du traitement à grande échelle

Le chiffre 24 de l'article 2 de la Loi n° 1.565 du 3 décembre, 2024 définit un traitement à grande échelle comme « *toute opération qui vise à traiter un **volume considérable de données** à caractère personnel, pouvant affecter un **nombre important de personnes concernées** apprécié en valeur absolue ou en valeur relative par rapport à la population concernée, et **susceptible d'engendrer un risque élevé**, compte tenu notamment de la **durée ou la permanence de l'activité** de traitement et de son **étendue géographique*** ».

A cet égard, l'Arrêté Ministériel n° 2025-361 du 14 juillet 2025 précise qu'une opération :

- visant à traiter un **volume considérable de données** et
- pouvant affecter un **nombre important de personnes concernées** (apprécié en valeur absolue ou en valeur relative par rapport à la population concernée) compte tenu notamment :
    - de la **durée ou la permanence** de l'activité et
    - de son **étendue géographique**

est susceptible d'engendrer **un risque élevé** dès lors :

- qu'elle remplit **au moins l'un des critères** visés à l'article premier de ce même arrêté (article 3 de l'Arrêté Ministériel n° 2025-361).

- qu'elle donne lieu à **l'utilisation d'un identifiant numérique** (article 4 de l'Arrêté Ministériel n° 2025-361).

Si le responsable du traitement estime qu'il est **peu probable que le traitement en question engendre un risque élevé** pour les droits et libertés des personnes physiques, et ne nécessite donc pas une analyse d'impact, il **doit être en mesure de le démontrer** (article 18 de l'Ordonnance Souveraine n° 11.327 du 10 juillet 2025 portant application de la loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles).

En cas de doute sur la nécessité d'effectuer une analyse d'impact, il est **recommandé d'en effectuer une malgré tout.** L'analyse d'impact est en effet un outil utile qui permet aux responsables du traitement **de s'assurer que les opérations envisagées respectent effectivement la protection des données personnelles.**

L'analyse d'impact n'est pas requise pour les traitements qui demeurent soumis à l'avis préalable de l'APDP ou de la Commission Spéciale de Sécurité Nationale instituée par l'article 16 de la Loi n° 1.430 du 13 juillet 2016.

Quand et comment doit être menée l'analyse d'impact ?

L'analyse d'impact doit être menée **avant la mise en œuvre du traitement** par **le responsable du traitement.**

S'il a désigné un **délégué à la protection des données**, le responsable du traitement doit lui demander **conseil** et le charger de **vérifier l'exécution** de l'analyse d'impact.

Par ailleurs, si un sous-traitant intervient dans le traitement, il doit fournir son **aide** et les **informations nécessaires** à la réalisation de l'analyse d'impact.

Une seule et même analyse d'impact peut porter sur un **ensemble d'opérations de traitement similaires dès lors que celles-ci présentent des risques élevés similaires**.

Le responsable du traitement doit en outre procéder une **réévaluation** de son analyse d'impact en cas de modification du risque.

Enfin, l'analyse d'impact doit être **conservée à titre probatoire** par le responsable du traitement et être communiquée **sur demande** à l'APDP.

Que doit contenir l'analyse d'impact ?

En vertu de l'article 35 de la Loi n° 1.565 du 3 décembre 2024, tout analyse d'impact doit *a minima* comporter les éléments suivants :

- une **description systématique des opérations de traitement envisagées et des finalités** du traitement, y compris, le cas échéant, **l'intérêt légitime poursuivi** par le responsable du traitement ;

- une évaluation de la nécessité et de la **proportionnalité des opérations de traitement au regard des finalités** ;

- une **évaluation des risques** pour les droits et libertés des personnes concernées ;

- **les mesures envisagées** pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection personnes concernées et des autres personnes affectées par les opérations de traitement envisagées.

Consultation préalable obligatoire de l'APDP en cas de risques résiduels élevés

Si lors de la réalisation de l'analyse d'impact, le responsable du traitement se rend compte que **les risques identifiés ne peuvent pas être suffisamment réduits** et qu'il existe des **risques résiduels élevés non maitrisés,** l'article 36 de la Loi n° 1.565 du 3 décembre 2024 prévoit qu'il **doit** consulter au préalable l'APDP.

Le responsable du traitement communique ainsi à l'Autorité les informations suivantes :

- les **responsabilités respectives** du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement et les coordonnées du délégué à la protection des données lorsque que celui-ci a été désigné ;

- **les finalités et les moyens** du traitement envisagé ;

- **les mesures et les garanties** prévues afin de protéger les droits et libertés des personnes concernées ;

- **l'analyse d'impact** qu'il a réalisée ;

- toute autre information demandée par l'Autorité.

L'APDP aura alors un délai maximum de 8 semaines pour rendre un **avis écrit** au responsable du traitement ; délai qui pourra être prolongé de 6 semaines en cas de traitements complexes.

Si l'Autorité considère que le traitement constitue en l'état une violation, elle imposera au responsable du traitement **les mesures appropriées** et pourra procéder aux **vérifications et investigations** prévues à l'article 46 de la Loi n° 1.565 du 3 décembre 2024.

Quelle est la sanction en cas de manquement aux exigences prévues en matière d'analyse d'impact ?

Tout manquement aux obligations en matière d'analyse d'impact, que ce soit l'obligation d'effectuer l'analyse d'impact en vertu de l'article 35 de la Loi n° 1.565 du 3 décembre 2024 ou l'obligation de consulter au préalable l'APDP en vertu de l'article 36 de la Loi n° 1.565 du 3 décembre 2024, est puni d'une amende administrative ne pouvant excéder **5.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu**.